

# Cyber-threat evolution: the past year

Costin Raiu, Kaspersky



Costin Raiu

It's time to sit back and take a look at what's been happening over the past 12 months in the IT security world. If we had to summarise the year in a single word, it would have to be 'explosive'. The multitude of incidents, stories, facts, new trends and intriguing actors is so big that it makes it very hard to come up with the top 10 security stories of 2011. The aim of this list is to remind ourselves of the stories that also indicated major trends or the emergence of new major actors on the security scene. By looking at these stories, we can get an idea of what will happen in 2012 – which we'll cover in the next article.

## The rise of 'hacktivism'

It's difficult to imagine someone reading this list who has not yet heard of Anonymous, LulzSec and maybe TeaMp0isoN. Throughout 2011, these groups, together with others, were actively involved in various operations against law enforcement agencies, banks, governments, security companies and major software vendors. Sometimes working together, in other cases working against each other, these groups emerged as one of the main groups of actors of 2011, through incidents such as security breaches of networks belonging to the United Nations, security intelligence firm Stratfor, FBI contractor IRC Federal, US defence contractor ManTech, and the CIA. Interestingly, some of these incidents, such as the Stratfor hack, revealed major security problems such as the storing of CVV numbers in unencrypted format, or extremely weak passwords used by administrators.

Overall, the rise of hacktivism was one of the major trends of 2011, and it is already continuing in 2012 with similar incidents.

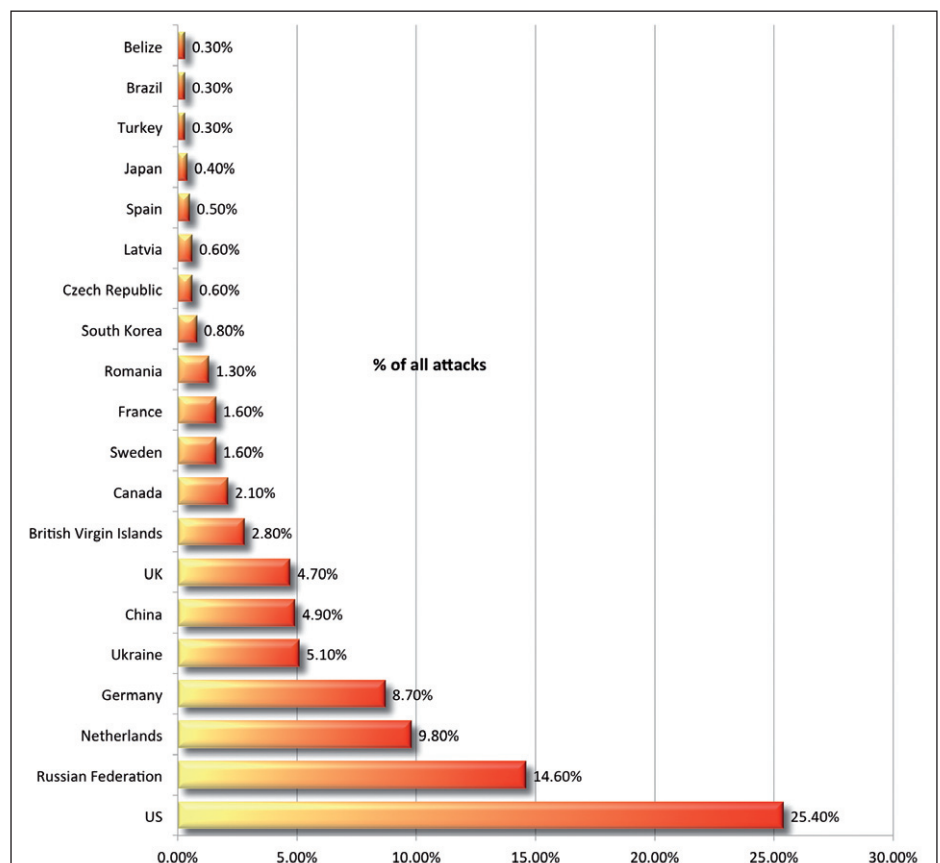
## The HBGary Federal hack

Although related to the first item on this list, this deserves to stand

alone as a separate story. In January 2011, hackers from the Anonymous activist collective broke into HBGary Federal's web server – hbgaryfederal.com – through a SQL injection attack. They were able to extract several MD5 hashes for passwords belonging to the company CEO, Aaron Barr, and COO

Ted Vera. Unfortunately, both used passwords that were very simple: six lowercase letters and two numbers. These passwords allowed the attackers to get access to the company's research documents and tens of thousands of mails stored on Google Apps.

This story is relevant because it demonstrates an interesting situation – the use of weak passwords together with old software systems plus use of the cloud can turn into a security nightmare. If the CEO and COO had used strong passwords, probably none of this would have happened. Or, if



The top 20 countries where web resources were seeded with malware. Servers seeded with malicious code were detected in the Internet zones of 198 countries around the world, but just 20 of those accounted for 89.4% of all malicious hosting detected by Kaspersky Lab.

they'd had multi-factor authentication enabled on Google Apps, the attackers wouldn't have been able to access the super-user account and copy all the company emails. It's important to point out that even if better security measures had been in place, we can't rule out the possibility that the ever-persistent hackers wouldn't have found another way in. Persistence and determination, combined with plenty of time, gives the attackers the upper hand.

## The Advanced Persistent Threat (APT)

Although many security experts despise this term, it has made its way into the media and rocketed to super-popularity with incidents such as the RSA security breach or the imposingly entitled incidents such as operations Night Dragon, Lurid and Shady Rat. Interestingly, many of these operations were not all that advanced at all. On the other hand, there were many cases in which zero-day exploits were used, such as in the RSA breach. In this case, the attackers took advantage of CVE-2011-0609 – a vulnerability in Adobe Flash Player – to run malicious code on the target machine. Another interesting zero-day was CVE-2011-2462, a vulnerability in Adobe Reader, that was used in targeted attacks against US defence contractor ManTech.

Several things stand out in these attacks:

- Many cases involved zero-day vulnerabilities in Adobe software.
- Many were directed at US targets, notably companies working with the US military or government.
- The Lurid attack was interesting because it mainly targeted countries in Eastern Europe such as Russia or CIS countries.

These attacks confirm the emergence of powerful nation-state actors and the establishment of cyber-espionage as common practice. Additionally, many of these attacks seemed to be

interconnected and have major global ramifications. For instance, the RSA breach was notable because the attackers stole the database of SecurID tokens, which was later used in another high-profile attack.

## The Comodo and DigiNotar incidents

On 15 March 2011 one of the affiliates of Comodo, a company known for its security software and SSL digital certificates, was hacked. The attacker quickly used the existing infrastructure to generate nine fake digital certificates for websites such as mail.google.com, login.yahoo.com, addons.mozilla.com and login.skype.com. During the analysis of the incident Comodo was able to identify the attacker as operating from the IP address 212.95.136.18 – in Tehran, Iran.

But in terms of size this was nothing compared to the DigiNotar breach. On 17 June 2011 hackers began poking around the DigiNotar servers, and over the next five days managed to get access to their infrastructure and generate over 300 fraudulent certificates. The hacker left a message in the form of a digital certificate containing a message in the Persian language: "Great hacker, I will crack all encryption, I break your head!" To make the link with Iran more solid, days later the fake certificates were used in a man-in-the-middle attack against over 100,000 Gmail users from Iran.

The attacks against Comodo and DigiNotar have highlighted that there's already been a loss of trust in the certificate authorities (CA). In the future, CA compromises may become more widespread. Besides, it is likely that more digitally signed malware will appear.

## Duqu

In June 2010, researcher Sergey Ulasen from the Belarusian company

VirusBlokada discovered an intriguing piece of malware that appeared to use stolen certificates to sign its drivers and a zero-day exploit that used .lnk files for replication in a typical Autorun fashion. This malware became world famous under the name Stuxnet, a computer worm containing a very special payload aimed directly at Iran's nuclear programme. Stuxnet hijacked Siemens Programmable Logic Controllers (PLCs) at Iran's Natanz plant and reprogrammed them in a very specific way, indicating one single objective: sabotaging the uranium enrichment process at Natanz. Back then, when I saw the code that reprogrammed the PLCs responsible for controlling the 64,000RPM centrifuges, I thought to myself that it's impossible to write something like that without having access to the original schematics and source code. But how could attackers have obtained something as sensitive as the custom code that controls the billion dollar facility?

***"Duqu and Stuxnet represent the state of the art in cyber-warfare and hint that we are entering an era of Cold Cyberwar"***

One possible answer lies within the Duqu trojan. Created by the same people that were responsible for Stuxnet, Duqu was discovered in August 2011 by the Hungarian research lab CrySyS. Originally, it wasn't known how Duqu infected its targets. Later, malicious Microsoft Word documents exploiting the vulnerability known as CVE-2011-3402 were discovered as a means of Duqu's penetration.

The purpose of Duqu is quite different from Stuxnet. This trojan is actually a sophisticated attack toolkit, which can be used to breach a system and then systematically siphon information out of it. New modules can be uploaded and run on the fly, without a file system footprint. The highly

modular architecture, together with the small number of victims around the world, made Duqu undetectable for years. The first trace of Duqu-related activity we were able to find actually dates back to August 2007. In all the incidents we have analysed, the attackers used an infrastructure of hacked servers to move the data – sometimes hundreds of megabytes – out of the victims' PCs.

Duqu and Stuxnet represent the state of the art in cyber-warfare and hint that we are entering an era of Cold Cyberwar, where superpowers fight each other unconstrained by the limitations of real-world war.

## The Sony PlayStation Network hack

On 19 April 2011, Sony learned that its PlayStation Network (PSN) had been hacked. At first the company was reluctant to explain what had happened and claimed that the service, which was suspended on April 20, would be back up in a few days. It wasn't until April 26 that the company acknowledged that personal information had been stolen, which potentially included credit card numbers. Three days later, reports appeared that seemed to indicate that 2.2 million credit card numbers were being offered for sale on hacker forums. By May 1, the PSN was still unavailable, which left many users not only having had their credit cards stolen but also frustrated at not being able to play the games they'd already paid for.

Then in October 2011, the PSN was again making the headlines with 93,000 compromised accounts that had to be locked down by Sony to prevent further misuse. The Sony PSN hack was a major story in 2011 because it indicates, among other things, that in the cloud era, Personally Identifiable Information (PII) is conveniently available in one place, accessed over fast Internet links, ready to be stolen in case of any misconfigurations or security issues. In 2011, 77 million

usernames and 2.2 million credit cards came to be considered normal 'booty' in the cloud era.

## Fighting cybercrime and botnet takedowns

While the attackers in the PSN incident are still unidentified, 2011 was a definitively bad year for the many cyber-criminals who got caught and arrested by law enforcement authorities around the world. The Zeus gang arrests, the DNSChanger gang takedown, and the Rustock, Coreflood and Kelihos/Hilux botnet takedowns were just a few examples.

***"A law enforcement agency could effectively push a program to all the infected users, notifying them in the process, or even cleaning their machines automatically"***

These indicate an emerging trend – bringing down a cyber-criminal gang goes a long way towards hampering criminal activity around the world, sending a message to the remaining gangs that this is no longer a risk-free undertaking. One particular case I'd like to mention is the Kelihos takedown, which was performed by Kaspersky Lab in co-operation with Microsoft's Digital Crimes Unit. Kaspersky Lab initiated a sinkhole operation for the botnet, counting many tens of thousands of infected users per day. And here's where the big debate starts: knowing the bot update process, Kaspersky Lab or a law enforcement agency could effectively push a program to all the infected users, notifying them in the process, or even cleaning their machines automatically. In a poll run on the Securelist website, a whopping 83% voted that Kaspersky Lab should "push a cleanup tool that removes the infections", despite this being illegal in most countries. For obvious reasons, we haven't done so,

but it outlines the limitations of today's legal system when it comes to fighting cybercrime in an effective manner.

## The rise of Android malware

In August 2010, Kaspersky identified the first trojan for the Android platform – Trojan-SMS.AndroidOS. FakePlayer.a – which masqueraded as a media player app. In less than a year, Android malware quickly exploded and became the most popular mobile malware category. This trend became obvious in the third quarter of 2011, in which we discovered over 40% of all the mobile malware we saw throughout the whole year. Finally, we hit critical mass in November 2011 when we uncovered over 1,000 malicious samples for Android, which is almost as many as all the mobile malware we have discovered in the past six years!

The huge popularity of Android malware can be attributed to several things – most notably the wild growth of Android itself. Second, the documentation freely available regarding the Android platform makes the creation of malware for Android quite easy. Finally, there are many who blame Google Market for its weak screening process, which makes it straightforward for cyber-criminals to upload malicious programs. While there are only two known malicious programs for the iPhone, we are now approaching 2,000 Android trojans already in our collection.

## The CarrierIQ incident

CarrierIQ is a small privately owned company, founded in 2005, and operating out of Mountain View, California. According to its website, CarrierIQ software is deployed on over 140 million devices around the world. Although the declared purpose of CarrierIQ is to collect 'diagnostic' information from mobile terminals, security researcher Trevor Eckhart

demonstrated how the extent of the information CarrierIQ collects goes beyond the declared simple diagnostic purpose, including things such as keylogging and monitoring URLs opened on a mobile device.

***“The CarrierIQ incident shows that we are totally unaware of what exactly is running on our mobile devices”***

CarrierIQ is built within a typical command and control architecture where system administrators can establish the kind of information that is collected from phones and which information is sent ‘home’. While it is obvious that CarrierIQ does collect a lot of information from your mobile phone, it doesn’t necessarily mean it is evil, or so we are advised to think by its creators – and companies such as HTC that support its use. However, being a US-based company, CarrierIQ could be forced to disclose much of the collected information to US law enforcement, if presented with a warrant. This legal loophole could effectively turn it into a government spy and monitoring tool. Whether this may indeed be the case, many users have decided that it’s best to get rid of CarrierIQ from their phones. Unfortunately, it isn’t a simple process and is different for iPhones, Android phones and BlackBerries. In the case of Android, you may have to root your phone in order to get rid of it. Alternatively, many users have decided to flash custom Android firmware instead, such as Cyanogenmod.

The CarrierIQ incident shows that we are totally unaware of what exactly is running on our mobile devices, or the level of control which the mobile operator has over our hardware.

## Mac malware

You put yourself into the line of fire by just mentioning Mac OS X malware,

but it’s an important story from 2011 that shouldn’t be overlooked. Products called MacDefender, MacSecurity, MacProtector or MacGuard, which are rogue anti-virus (AV) products for Mac OS, appeared in May 2011 and quickly became popular. Distributed through black-hat SEO techniques in Google searches, these programs rely on social engineering to get the user to download, install, and then pay for the ‘full’ version. Most of those who decide to pay \$40 for the supposedly full version later discover that they actually paid \$140, and sometimes they paid several times over.

The crossing over of PC threats (rogue AV programs being one of the most popular malware categories for PCs) to Macs was an important trend in 2011. In addition to OS X rogue AVs, the DNSChanger family of trojans deserves special mention as well. First identified around 2007, these small trojans conduct a very simple and straightforward system compromise by changing the DNS settings to point to the criminals’ private DNS servers, before uninstalling themselves. Hence, you may get infected with a DNSChanger, have your DNS settings changed, and think you’re fine because there’s no malware actually on your computer. In reality what the criminals do is abuse the DNS communication to make you visit fake websites and perform click fraud and man-in-the-middle attacks. Luckily, in November 2011, the FBI arrested the six Estonian nationals who made up the gang behind the DNSChanger malware. According to FBI data, in the past four years they infected over four million computers in more than 100 countries and generated approximately \$14 million in illegal profits. These incidents show that malware for OS X is as real as malware for PCs, and that even modern security practices fail against carefully elaborated social engineering techniques. It is without doubt that we

will see both platforms continue to be abused in the future.

## Summary

To summarise, these 10 stories are just a tiny speck in the galaxy of 2011 security incidents. The reason they were selected is because they point to the major actors of 2011 who will no doubt continue to play a major role in the cyber-security blockbuster that is around the corner. These are the hacktivist groups; the security companies; the advanced persistent threat in the form of superpowers fighting each other through cyber-espionage; the major software and gaming developers such as Adobe, Microsoft, Oracle and Sony; law enforcement agencies; traditional cyber-criminals; Google – via the Android operating system; and Apple – thanks to its OS X platform. The relations among these can be complicated, full of drama and contain many super-secret details. One thing is for sure – these same stars will be playing in all the major 2012 security blockbuster movies.

## About the author

*Costin Raiu is director of the Global Research & Analysis Team at Kaspersky Lab. He joined the company in 2000 as a leading anti-virus researcher. Prior to his current post he was head of the Romanian R&D group, overseeing research efforts in the EEMEA region. Raiu specialises in malicious websites, browser security and exploits, e-banking malware, enterprise-level security and Web 2.0 threats. He also has a particular interest in encryption and advanced mathematics. Raiu has extensive experience in anti-virus technologies and security research. He is a member of the Virus Bulletin Technical Advisory Board and a reporter for the Wildlist Organisation International. Prior to joining Kaspersky Lab, he worked for GeCad as one of its chief researchers and as a data security expert with the RAV anti-virus developers group.*